Gröbner-Shirshov basis for HNN extensions of groups and for the alternating group *

Yuqun Chen and Chanyan Zhong

School of Mathematical Sciences
South China Normal University
Guangzhou 510631
P. R. China
yqchen@scnu.edu.cn
zhongchanyan@tom.com

Abstract: In this paper, we generalize the Shirshov's Composition Lemma by replacing the monomial order for others. By using Gröbner-Shirshov bases, the normal forms of HNN extension of a group and the alternating group are obtained.

Key words: Gröbner-Shirshov basis, normal form, HNN extension, alternating group

AMS Mathematics Subject Classification(2000): 20E06, 16S15, 13P10

1 Preliminaries

It is known that in the Gröbner-Shirshov basis theory, the Shirshov's Composition-Diamond Lemma [19] plays an important role. In the Composition-Diamond Lemma, the order is asked to be monomial. In this paper, we generalize the Composition-Diamond Lemma by replacing the monomial order for others. From this result, we show by direct calculations of compositions, that the presentation of the HNN extension is a Gröbner-Shirshov basis under an appropriate ordering of group words, in which the order is not monomial order. By the generalized composition lemma, we immediately obtain the Normal Form Theorem for HNN extensions. In fact, this is the first time to find a Gröbner-Shirshov basis by using a non-monomial order.

HNN extensions of groups were first invented by Higman-Neumann-Neumann in 1949 ([12]) and independently by P. S. Novikov in 1952 (see [16], [17], [18]). The Normal Form Theorem for certain HNN extensions of groups was first established by L. A. Bokut (see [2], [3], [4] and see also K. Kalorkoti [14]). In general, the Normal Form Theorem for HNN extensions of groups was proved in the text of Lyndon-Schupp [15].

For the alternating group A_n, a presentation was given in the monograph of N. Jacobson (see [13], p71). However, we still do not know what is the normal form for A_n. In

*The research is supported by the National Natural Science Foundation of China (Grant No.10771077) and the Natural Science Foundation of Guangdong Province (Grant No.06025062).

this paper, we give the normal form theorem of A_n with respect to the above presentation.

We first cite some concepts and results from the literature. Let k be a field, $k\langle X\rangle$ the free associative algebra over k generated by X and X^* the free monoid generated by X, where the empty word is the identity which is denoted by 1. For a word $w \in X^*$, we denote the length of w by $deg(w)$. Let X^* be a well ordered set. Let $f = \sum_{a\in X^*} f(a)a \in k\langle X\rangle$, where $f(a) \in k$, with the leading word $\bar{f}$. We say that f is monic if $\bar{f}$ has coefficient 1. We denote $suppf = \{a \in X^* | f(a) \neq 0\}$.

Definition 1.1 *([19], see also [5], [6]) Let f and g be two monic polynomials in $k\langle X\rangle$. Then, there are two kinds of compositions:*

(1) If w is a word such that $w = \bar{f}b = a\bar{g}$ for some $a, b \in X^*$ with $deg(\bar{f})+deg(\bar{g}) > deg(w)$, then the polynomial $(f, g)_w = fb - ag$ is called the intersection composition of f and g with respect to w.

(2) If $w = \bar{f} = a\bar{g}b$ for some $a, b \in X^*$, then the polynomial $(f, g)_w = f - agb$ is called the inclusion composition of f and g with respect to w.

In the above case, the transformation $f \mapsto (f, g)_w = f - agb$ is called the elmination of the leading word (ELW) of g in f.

Definition 1.2 *([5], [6], cf. [19]) Let $S \subseteq k\langle X\rangle$ and $<$ a well order on X^*. Then the composition $(f, g)_w$ is called trivial modulo S if $(f, g)_w = \sum \alpha_i a_i s_i b_i$, where each $\alpha_i \in k$, $a_i, b_i \in X^*$ and $\overline{a_i s_i b_i} < w$. If this is the case, then we write*

$$(f, g)_w \equiv 0 \quad mod(S, w)$$

In general, for $p, q \in k\langle X\rangle$, we write

$$p \equiv q \quad mod(S, w)$$

which means that $p - q = \sum \alpha_i a_i s_i b_i$, where each $\alpha_i \in k, a_i, b_i \in X^*$ and $\overline{a_i s_i b_i} < w$.

Definition 1.3 *([5], [6], cf. [19]) We call the set S with respect to the well order "$<$" a Gröbner-Shirshov set (basis) in $k\langle X\rangle$ if any composition of polynomials in S is trivial modulo S.*

Remark: Usually, in the definition of the Gröbner-Shirshov basis, the order is asked to be monomial.

A well order "$<$" on X^* is monomial if it is compatible with the multiplication of words, that is, for $u, v \in X^*$, we have

$$u > v \Rightarrow w_1 u w_2 > w_1 v w_2, \ for\ all\ w_1,\ w_2 \in X^*.$$

The following lemma was proved by Shirshov [19] for the free Lie algebras (with deg-lex ordering) in 1962 (see also Bokut [5]). In 1976, Bokut [6] specialized the approach of Shirshov to associative algebras (see also Bergman [1]). For commutative polynomials, this lemma is known as the Buchberger's Theorem (see [10]), published in [11].

Lemma 1.4 *(Composition-Diamond Lemma) Let $A = k\langle X|S\rangle$ and " $<$ " a monomial order on X^*. Then the following statements are equivalent:*

(i) S is a Gröbner-Shirshov basis.

(ii) For any $f \in k\langle X\rangle$, $0 \neq f \in Ideal(S) \Rightarrow \bar{f} = a\bar{s}b$ for some $s \in S$, $a, b \in X^*$.

(iii) The set

$$Red(S) = \{u \in X^* | u \neq a\bar{s}b, s \in S, a, b \in X^*\}$$

is a linear basis of the algebra A.

If a subset S of $k\langle X\rangle$ is not a Gröbner-Shirshov basis, then we can add to S all nontrivial compositions of polynomials of S, and by continuing this process (maybe infinitely) many times, we eventually obtain a Gröbner-Shirshov basis S^{comp}. Such a process is called the Shirshov algorithm.

If S is a set of "semigroup relations" (that is, the polynomials of the form $u - v$, where $u, v \in X^*$), then any nontrivial composition will have the same form. As a result, the set S^{comp} also consists of semigroup relations.

Let $A = sgp\langle X|S\rangle$ be a semigroup presentation. Then S is a subset of $k\langle X\rangle$ and hence one can find a Gröbner-Shirshov basis S^{comp}. The last set does not depend on k, and as mentioned before, it consists of semigroup relations. We will call S^{comp} a Gröbner-shirshov basis of A. This is the same as a Gröbner-shirshov basis of the semigroup algebra $kA = k\langle X|S\rangle$.

2 Generalized Composition-Diamond Lemma

In this section, we generalize the Composition-Diamond Lemma which is useful in the sequel, by replacing the monomial order for others. The proof of the following lemma is essentially the same as in [7]. For the sake of convenience, we give the details.

Lemma 2.1 *(Generalized Composition-Diamond Lemma) Let $S \subseteq k\langle X\rangle$, $A = k\langle X|S\rangle$ and " $<$ " a well order on X^* such that*

(A) $\overline{asb} = a\bar{s}b$ for any $a, b \in X^*$, $s \in S$;

(B) for each composition $(s_1, s_2)_w$ in S, there exists a presentation

$$(s_1, s_2)_w = \sum_i \alpha_i a_i t_i b_i,\ a_i \bar{t}_i b_i < w, \quad \text{where } t_i \in S,\ a_i, b_i \in X^*,\ \alpha_i \in k$$

such that for any $c, d \in X^*$, we have

$$c a_i \bar{t}_i b_i d < cwd \tag{1}$$

Then, the following statements hold.

(i) S is a Gröbner-Shirshov basis.

(ii) *For any* $f \in k\langle X\rangle,\ 0 \neq f \in Ideal(S) \Rightarrow \bar{f} = a\bar{s}b$ *for some* $s \in S,\ a, b \in X^*$.

(iii) *The set*

$$Red(S) = \{u \in X^* | u \neq a\bar{s}b, s \in S, a, b \in X^*\}$$

is a linear basis of the algebra A.

Proof (i) is clear. Now, we prove (ii). Let

$$f = \sum_{i=1}^{n} \alpha_i a_i s_i b_i,\ \alpha_i \in k,\ s_i \in S,\ a_i, b_i \in X^*$$

Assume that

$$w_i = a_i \bar{s_i} b_i,\ w_1 = w_2 = \cdots = w_l > w_{l+1} \cdots$$

We will use the induction on l and w_1 to prove that $\bar{f} = a\bar{s}b$, for some $s \in S$ and $a, b \in X^*$.

If $l = 1$, then by (A), $\bar{f} = a_1\bar{s_1}b_1$ and hence the result holds. Assume that $l \geq 2$. Then

$$f = (\alpha_1 + \alpha_2)a_1s_1b_1 + \alpha_2(a_2s_2b_2 - a_1s_1b_1) + \cdots$$

For $w_1 = w_2$, there are three cases to consider.

Case 1. Assume that $b_1 = b\bar{s_2}b_2$ and $a_2 = a_1\bar{s_1}b$. Then we have

$$a_2s_2b_2 - a_1s_1b_1 = a_1s_1b(s_2 - \bar{s_2})b_2 - a_1(s_1 - \bar{s_1})bs_2b_2.$$

For any $t \in supp(s_2 - \bar{s_2})$, by (A), $\overline{a_1s_1btb_2} = a_1\bar{s_1}btb_2 < a_1\bar{s_1}b\bar{s_2}b_2 = w_1$ and similarly, we have $\overline{a_1t_1bs_2b_2} < w_1$, for any $t_1 \in supp(s_1 - \bar{s_1})$.

Case 2. Assume that $b_1 = bb_2,\ a_2 = a_1a,\ \bar{s_1}b = a\bar{s_2}$ and $deg\bar{s_1} + deg\bar{s_2} > deg(a\bar{s_1})$. Then

$$a_2s_2b_2 - a_1s_1b_1 = a_1(as_2 - s_1b)b_2.$$

By (B), there exist $\beta_j \in k,\ u_j, v_j \in X^*,\ t_j \in S$ such that $u_j\bar{t_j}v_j < w = \bar{s_1}b,\ s_1b - as_2 = \sum_j \beta_j u_j t_j v_j$ and $a_1u_j\bar{t_j}v_jb_2 < a_1\bar{s_1}bb_2$. Now, by (A), for any j, we have $\overline{a_1u_jt_jv_jb_2} = a_1u_j\bar{t_j}v_jb_2 < a_1\bar{s_1}bb_2 = w_1$.

Case 3. Assume that $b_2 = bb_1,\ a_2 = a_1a$ and $\bar{s_1} = a\bar{s_2}b$. Then

$$a_2s_2b_2 - a_1s_1b_1 = a_1(as_2b - s_1)b_1.$$

by (A) and (B), there exist $\beta_j \in k,\ u_j, v_j \in X^*,\ t_j \in S$ such that $u_j\bar{t_j}v_j < w = \bar{s_1},\ s_1 - as_2b = \sum_j \beta_j u_j t_j v_j$ and for any j, we have $\overline{a_1u_jt_jv_jb_1} = a_1u_j\bar{t_j}v_jb_1 < a_1\bar{s_1}b_1 = w_1$.

(iii) follows from (ii). $\square$

3 Normal form for HNN extension of group

In this section, by using the Gröbner-Shirshov basis, we provide a new proof of the normal form theorem of HNN extension of a group.

Definition 3.1 *([12],[16],[17],[18]) Let* G *be a group and let* A *and* B *be subgroups of* G *with* $\phi : A \to B$ *an isomorphism. Then the HNN extension of* G *relative to* A *,* B *and* ϕ *is the group*

$$\mathcal{G} = gp\langle G, t; t^{-1}at = \phi(a), a \in A\rangle.$$

Let $G = G_1 \cup \{1\}$, where $G_1 = G \setminus \{1\} = \{g_\alpha; \alpha \in \Lambda\}$, and let

$$G/A = \{g_i A; i \in I\},\ G/B = \{h_j B; j \in J\},$$

where $\{g_i; i \in I\}$ and $\{h_j; j \in J\}$ are the coset representatives of A and B in G, respectively. We assume that all sets $\Lambda,\ I,\ J$ are well ordered and so are the sets $\{g_\alpha; \alpha \in \Lambda\},\ \{g_i; i \in I\},\ \{h_j; j \in J\}$. Then we get a new presentation of the group $\mathcal{G}$ as a semigroup:

$$\begin{aligned} \mathcal{G} = sgp\langle G_1, t, t^{-1} \quad ; \quad & gg' = [gg'], gt = g_{_A} t\phi(a_g), gt^{-1} = g_{_B} t^{-1}\phi^{-1}(b_g), \\ & t^{\varepsilon} t^{-\varepsilon} = 1,\ g, g' \in G_1,\ \varepsilon = \pm 1\rangle, \end{aligned}$$

where $[gg'] \in G;\ g = g_{_A} a_g,\ g_{_A} \in \{g_i; i \in I\},\ g \neq g_{_A},\ a_g \in A;\ g = g_{_B} b_g,\ g_{_B} \in \{h_j; j \in J\},\ g \neq g_{_B},\ b_g \in B$.

Now, we order the set G in three different ways:

(1) Let $1 < g_{_\alpha} < g_{_\beta} < \cdots\ (\alpha < \beta)$ be a well order of G. Then we denote this order by $(G, >)$ and call it an absolute order.

(2) For any $g, g' \in G$, suppose that $g = g_{_A} a_g, g' = g'_{_A} a_{g'}$. Then $g >_{_A} g'$ if and only if $(g_{_A}, a_g) > (g'_{_A}, a'_g)$ is ordered lexicographically (elements $g_{_A}, g'_{_A}$ by I, elements $a_g, a_{g'}$ by (1)). We denote this order by $(G, >_{_A})$ and call it the A-order. In particular, if $g \neq g_{_A}$, then $g >_{_A} g_{_A}$, for $(g_{_A}, a_g) > (g_{_A}, 1),\ a_g \neq 1$.

(3) For any $g, g' \in G$, suppose that $g = g_{_B} b_g, g' = g'_{_B} b_{g'}$. Then $g >_{_B} g'$ if and only if $(g_{_B}, b_g) > (g'_{_B}, b'_g)$ is ordered lexicographically (elements $g_{_B}, g'_{_B}$ by J, elements $b_g, b_{g'}$ by (1)). We denote this order by $(G, >_{_B})$ and call it the B-order.

Then we order the set G_1^* in three different ways too:

(1) The absolute order $({G_1}^*, \leq)$ is deg-lex order, to compare words $g_1 \cdots g_n\ (n \geq 0)$ first by length and then lexicographically using absolute order of G_1.

(2) The A-order $({G_1}^*, \leq_{_A})$ is $deg-lex_{_A}$ order, firstly to compare words $g_1 \cdots g_n\ (n \geq 0)$ by length, secondly for $n \geq 1,\ g_1, \cdots, g_{n-1}$ lexicographically by absolute order, and finally the last elements g_n by A-order.

(3) The B-order $({G_1}^*, \leq_{B})$ is similar to (2) replacing $>_{_A}$ by $>_{_B}$.

Each element in $\{G_1 \dot\cup \{t, t^{-1}\}\}^*$ has a unique form $u = u_1 t^{\varepsilon_1} u_2 t^{\varepsilon_2} \cdots u_k t^{\varepsilon_k} u_{k+1}$, where each $u_i \in G_1^*, \varepsilon_i = \pm 1,\ k \geq 0$. Suppose that $v = v_1 t^{\delta_1} v_2 \cdots v_l t^{\delta_l} v_{l+1} \in \{G_1 \dot\cup \{t, t^{-1}\}\}^*$.

Then

$$wt(u) = (k, t^{\varepsilon_1}, \cdots, t^{\varepsilon_k}, u_1, \cdots, u_k, u_{k+1})$$

$$wt(v) = (l, t^{\delta_1}, \cdots, t^{\delta_l}, v_1, \cdots, v_l, v_{l+1})$$

We define $u \succ v$ if $wt(u) > wt(v)$ lexicographically, using the order of natural numbers and the following orders:

(a) $t > t^{-1}$

(b) $u_i >_{A} v_i$ if $\varepsilon_i = 1,\ 1 \leq i \leq k$

(c) $u_i >_{B} v_i$ if $\varepsilon_i = -1,\ 1 \leq i \leq k$

(d) $u_{k+1} > v_{l+1}$ $(k = l)$, the absolute order of ${G_1}^*$

Now, we can easily verify the following lemma.

Lemma 3.2 *Let the order $\succ$ on $\{G_1\dot{\cup}\{t, t^{-1}\}\}^*$ be defined as above. Then the order $\succ$ is a well order but not monomial, for example, $g \succ g'$ does not necessarily imply that $gt \succ g't$.*

Equipping with the above notation, we have the following lemma.

Lemma 3.3 *Let $X = G_1\dot{\cup}\{t, t^{-1}\}$. Suppose that the order $\succ$ on X^* is defined as above and $S = \{gg' - [gg'],\ gt - g_{A}t\phi(a_g),\ gt^{-1} - g_{B}t^{-1}\phi^{-1}(b_g),\ t^{\varepsilon}t^{-\varepsilon} - 1 \mid g, g' \in G_1,\ \varepsilon = \pm 1\}$ is as above too. Then S satisfies conditions (A)-(B) in Lemma 2.1.*

Proof For any $c, d \in X^*$, suppose that $c = c_1t^{\varepsilon_1}\cdots c_nt^{\varepsilon_n}c_{n+1},\ d = d_1t^{\delta_1}\cdots d_mt^{\delta_m}d_{m+1},\ c_i, d_j \in G_1^*,\ \varepsilon_i, \delta_j = \pm 1$. We firstly check (A). Then there are four cases to consider. For example, the second case is for polynomials $gt - g_{A}t\phi(a_g),\ g \neq g_{A}$. We need to prove that $cgtd \succ cg_At\phi(a_g)d$ for any c, d.

Since

$$\begin{aligned} wt(cgtd) &= (n+m+1, t^{\varepsilon_1}, \cdots, t^{\varepsilon_n}, t, t^{\delta_1}, \cdots, t^{\delta_m}, c_1, \cdots, c_n, c_{n+1}g, \\ &\quad\ d_1, \cdots, d_m, d_{m+1}), \\ wt(cg_{A}t\phi(a_g)d) &= (n+m+1, t^{\varepsilon_1}, \cdots, t^{\varepsilon_n}, t, t^{\delta_1}, \cdots, t^{\delta_m}, c_1, \cdots, c_n, c_{n+1}g_{A}, \\ &\quad\ \phi(a_g)d_1, \cdots, d_m, d_{m+1}) \end{aligned}$$

and $c_{n+1}g >_{A} c_{n+1}g_{A}$ (since $g >_{A} g_{A}$), we have $cgtd \succ cg_At\phi(a_g)d$.

We secondly check that (B) holds in Lemma 2.1. By noting that there is no inclusion compositions in S, we need only to consider the cases of intersection compositions. For any $a, b \in X^*,\ s_1, s_2 \in S$, suppose that $a\bar{s_1} = \bar{s_2}b$ with $deg\bar{s_1} + deg\bar{s_2} > deg(a\bar{s_1})$. Then, we consider the following cases:

$$w = gg'g'',\ gg't\ (g' \neq g'_{A}),\ gg't^{-1}\ (g' \neq g'_{B}),\ gt^{\varepsilon}t^{-\varepsilon},\ t^{\varepsilon}t^{-\varepsilon}t^{\varepsilon}\ (\varepsilon = \pm 1).$$

For example, the second case is as follows:

Let $\bar{s_1} = gg',\ \bar{s_2} = g't,\ w = gg't$. Then, by noting that $gg' = [gg']_{A}a_{[gg']} = [gg'_{A}]_{A}a_{[gg'_{A}]}a_{g'}$ implies that $[gg']_{A} = [gg'_{A}]_{A}$ and $a_{[gg']} = a_{[gg'_{A}]}a_{g'}$, we know that $(s_2, s_1)_w = [gg']t - gg'_{\ A}t\phi(a_{g'}) = ([gg']t - [gg']_{A}t\phi(a_{[gg']})) - (gg'_{A} - [gg'_{A}])t\phi(a_{g'}) - ([gg'_{\ A}]t\phi(a_{g'}) - [gg'_{A}]_{A}t\phi(a_{[gg'_{A}]}a_{g'}))$. We denote $s'_1 = [gg']t - [gg']_{A}t\phi(a_{[gg']}),\ s'_2 = gg'_{A} - [gg'_{A}],\ b_2 = t\phi(a_{g'}),\ s'_3 = [gg'_{\ A}]t\phi(a_{g'}) - [gg'_{A}]_{A}t\phi(a_{[gg'_{A}]}a_{g'})$. Clearly, $s'_1,\ s'_2,\ s'_3 \in S$ or $\{0\}$ (if

$[gg'] = [gg']_{_A})$. Since

$$\begin{aligned} wt(c\bar{s_1'}d) &= (n+m+1, t^{\varepsilon_1}, \cdots, t^{\varepsilon_n}, t, t^{\delta_1}, \cdots, t^{\delta_m}, c_1, \cdots, c_n, c_{n+1}[gg'], \\ & \quad d_1, \cdots, d_m, d_{m+1}), \\ wt(c\bar{s_2'}b_2d) &= (n+m+1, t^{\varepsilon_1}, \cdots, t^{\varepsilon_n}, t, t^{\delta_1}, \cdots, t^{\delta_m}, c_1, \cdots, c_n, c_{n+1}gg'_{_A}, \\ & \quad \phi(a_{g'})d_1, \cdots, d_m, d_{m+1}), \\ wt(c\bar{s_3'}d) &= (n+m+1, t^{\varepsilon_1}, \cdots, t^{\varepsilon_n}, t, t^{\delta_1}, \cdots, t^{\delta_m}, c_1, \cdots, c_n, c_{n+1}[gg'_{_A}], \\ & \quad \phi(a_{g'})d_1, \cdots, d_m, d_{m+1}), \\ wt(cwd) &= (n+m+1, t^{\varepsilon_1}, \cdots, t^{\varepsilon_n}, t, t^{\delta_1}, \cdots, t^{\delta_m}, c_1, \cdots, c_n, c_{n+1}gg', \\ & \quad d_1, \cdots, d_m, d_{m+1}) \end{aligned}$$

and $c_{n+1}gg' >_{_A} c_{n+1}[gg'],\ c_{n+1}gg'_{_A},\ c_{n+1}[gg'_{_A}]$, we have $cwd \succ c\bar{s_1'}d,\ c\bar{s_2'}b_2d,\ c\bar{s_3'}d$. All other cases are treated the same. The proof is finished. $\square$

Now, by Lemma 2.1 and Lemma 3.3, we obtain the following theorem.

Theorem 3.4 *A Gröbner-Shirshov basis of HNN extention $\mathcal{G} = gp\langle G, t; t^{-1}at = \phi(a), a \in A\rangle$ consists of the following relations:*

(3.1) $gg' = [gg']$;

(3.2) $gt = g_{_A}t\phi(a_g)$, *where* $g = g_{_A}a_g,\ g_{_A} \in \{g_i, i \in I\},\ a_g \in A$;

(3.3) $gt^{-1} = g_{_B}t^{-1}\phi^{-1}(b_g)$, *where* $g = g_{_B}b_g,\ g_{_B} \in \{h_j, j \in J\},\ b_g \in B$;

(3.4) $tt^{-1} = 1,\ t^{-1}t = 1.$

where $\{g_i; i \in I\}$ and $\{h_j; j \in J\}$ are the coset representatives of A and $B = \phi(A)$ in G, respectively.

Thus S is a Gröbner-Shirshov basis of the algebra $k\langle G_1\dot{\cup}\{t, t^{-1}\}\rangle$ with

$$Red(S) = \{u \in \{G_1\dot{\cup}\{t, t^{-1}\}\}^* | u \neq a\bar{s}b, s \in S, a, b \in \{G_1\dot{\cup}\{t, t^{-1}\}\}^*\}$$

which is the normal form of the HNN extension $\mathcal{G}$. From this result, the normal form theorem for HNN Extension of the Group G easily follows.

Theorem 3.5 *(The Normal Form Theorem for HNN Extension, [15], Theorem 4.2.1) Let $\mathcal{G} = gp\langle G, t; t^{-1}at = \phi(a), a \in A\rangle$ be an HNN extension of group G. If $\{g_i; i \in I\}$, and $\{h_j; j \in J\}$ are the sets of representatives of the left cosets of A and $B = \phi(A)$ in G, respectively, then every element w of $\mathcal{G}$ has a unique representation $w = g_1t^{\varepsilon_1}\cdots g_nt^{\varepsilon_n}g_{n+1}$ $(n \geq 0,\ \varepsilon_l = \pm 1)$, where, for $1 \leq l \leq n$, the following conditions are satisfied:*

(1) *if* $\varepsilon_l = 1$, *then* $g_l \in \{g_i; i \in I\}$,

(2) *if* $\varepsilon_l = -1$, *then* $g_l \in \{h_j; j \in J\}$,

(3) there does not exist subwords tt^{-1} and $t^{-1}t$,

(4) g_{n+1} is an arbitrary element of G.

Remark: In Theorem 4.2.1 of [15], the right cosets were considered. We notice that the above Theorem 3.5 is essentially the same as Theorem 4.2.1 in [15].

4 Normal form for alternating group

In this section, we first find a Gröner-Shirshov basis for the alternating group A_n and then we give the normal form theorem of A_n.

Let S_n be the group of the permutations of $\{1, 2, \cdots, n\}$. Then the subset A_n of all even permutations in S_n is a normal subgroup of S_n. We call A_n the alternating group of degree n. The following presentation of A_n was given in the monograph of N. Jacobson (see [13], p71):

$$\begin{aligned} A_n = gp\langle x_i \ (1 \le i \le n-2) \quad ; \quad & x_1^3 = 1, \ (x_{i-1}x_i)^3 = x_i^2 = 1 \ (2 \le i \le n-2), \\ & (x_i x_j)^2 = 1 \ (1 \le i < j-1, j \le n-2)\rangle \end{aligned}$$

where $x_i = (12)((i+1)(i+2)), \ i = 1, 2, \cdots, n-2, \ (ij)$ the transposition. We now give a presentation of the group A_n as a semigroup:

$$\begin{aligned} A_n \ = \ & sgp\langle x_1^{-1}, \ x_i \ (1 \le i \le n-2); \ x_1 x_1^{-1} = x_1^{-1} x_1 = x_1^3 = 1, \ (x_{i-1}x_i)^3 = x_i^2 = 1 \\ & (2 \le i \le n-2), \ (x_i x_j)^2 = 1 \ (1 \le i < j-1, j \le n-2)\rangle \end{aligned}$$

We now order the generators in the following way:

$$x_1^{-1} < x_1 < x_2 < \cdots < x_{n-2}$$

Let $X = \{x_1^{-1}, x_1, x_2, \cdots, x_{n-2}\}$. Then, with the above notations, we can order the words of X^* by the deg-lex order, i.e., compare two words first by their degrees, then order them lexicographically when the degrees are equal. Clearly, this order is a monomial order. Now we define the words

$$x_{ji} = x_j x_{j-1} ... x_i,$$

where $j > i > 1$ and $x_{j1\varepsilon} = x_j x_{j-1} ... {x_1}^{\varepsilon}, \varepsilon = \pm 1$.

The proof of the following lemma is straightforward. We omit the details.

Lemma 4.1 *For $\varepsilon = \pm 1$, the following relations hold in the alternating group A_n:*

(4.1) $x_1^{2\varepsilon} = x_1^{-\varepsilon}$

(4.2) $x_i^2 = 1, (i > 1)$

(4.3) $x_j x_i = x_i x_j, (j - 1 > i \ge 2)$

(4.4) $x_j x_1^{\varepsilon} = x_1^{-\varepsilon} x_j, (j > 2)$

(4.5) $x_{ji}x_j = x_{j-1}x_{ji}, (j > i \geq 2)$

(4.6) $x_{j1\varepsilon}x_j = x_{j-1}x_{j1-\varepsilon}, (j > 2)$

(4.7) $x_2{x_1}^{\varepsilon}x_2 = x_1^{-\varepsilon}x_2x_1^{-\varepsilon}$

(4.8) $x_1^{\varepsilon}x_1^{-\varepsilon} = 1$

Now, we can state the normal form theorem for the group A_n.

Theorem 4.2 *Let*

$$A_n = gp\langle x_i \ (1 \leq i \leq n-2) \ ; \ x_1^3 = 1, \ (x_{i-1}x_i)^3 = {x_i}^2 = 1 \ (2 \leq i \leq n-2), \ (x_ix_j)^2 = 1 \ (1 \leq i < j-1, j \leq n-2)\rangle$$

be the alternating group of degree n*. Let* $S = \{x_1^{2\varepsilon} - x_1^{-\varepsilon}, \ x_i^2 - 1 \ (i > 1), \ x_jx_i - x_ix_j \ (j-1 > i \geq 2), \ x_jx_1^{\varepsilon} - x_1^{-\varepsilon}x_j \ (j > 2), \ x_{ji}x_j - x_{j-1}x_{ji} \ (j > i \geq 2), \ x_{j1\varepsilon}x_j - x_{j-1}x_{j1-\varepsilon} \ (j > 2), \ x_2{x_1}^{\varepsilon}x_2 - x_1^{-\varepsilon}x_2x_1^{-\varepsilon}, \ x_1^{\varepsilon}x_1^{-\varepsilon} - 1, \ \varepsilon = \pm 1\}$*, where* $x_{ji} = x_jx_{j-1}...x_i, \ j > i > 1, \ x_{i1\varepsilon} = x_ix_{i-1}...{x_1}^{\varepsilon}, \ \varepsilon = \pm 1$*. Then*

(i) S *is a Gröbner-Shirshov basis of the alternating group* A_n*;*

(ii) every element w *of* A_n *has a unique representation* $w = x_{1j_1}x_{2j_2}...x_{n-2j_{n-2}}$*, where* $x_{tt} = x_t \ (t > 1), \ x_{ii+1} = 1, \ x_{i1} = x_ix_{i-1}\cdots x_1^{\varepsilon}, \ 1 \leq j_i \leq i+1, \ 1 \leq i \leq n-2, \ \varepsilon = \pm 1$ *(here we use* x_{i1} *instead of* $x_{i1\varepsilon}$*).*

Proof By Lemma 4.1, it is easy to see that every element w of A_n has a representation $w = x_{1j_1}x_{2j_2}...x_{n-2j_{n-2}} \ (j_i \leq i+1)$. Here x_{1j_1} may have 3 possibilities $1, x_1, x_1^{-1}$; x_{2j_2} 4 possibilities, and generally, x_{ij_i} $i+2$ possibilities, $1 \leq i \leq n-2$. So there are $n!/2$ words. From this fact, it follows that each representation is unique since $|A_n| = n!/2$. On the other hand, it is clear that $Red(S)$ consists of the same words w. Hence, by Composition-Diamond Lemma, S is a Gröbner-Shirshov basis of the alternating group A_n. $\square$

Remark: According to [8], normal form in S_{n-1} is $x_{1j_1}x_{2j_2}...x_{n-2j_{n-2}}$, but here $x_{i1} = x_ix_{i-1}\cdots x_1$.

Acknowledgement: The authors would like to express their deepest gratitude to Professor L. A. Bokut for his kind guidance, useful discussions and enthusiastic encouragement during his visit to the South China Normal University.

References

[1] G. M. Bergman, The diamond lemma for ring theory, *Adv. in Math.*, 29, 178-218(1978).

[2] L. A. Bokut, On one property of the Boone group, *Algebra i Logika*, 5(5), 5-23(1966); II, 6(1), 25-38(1967).

[3] L. A. Bokut, On the Novikov groups, *Algebra i Logika*, 6(1), 25-38(1967).

[4] L. A. Bokut, Degrees of unsolvability of the conjugacy problems for finitele presented groups, I, II, *Algebra i Logika*, 7(5), 4-70(1968); 7(6), 4-52(1968).

[5] L. A. Bokut, Unsolvability of the word problem, and subalgebras of finitely presented Lie algebras, *Izv. Akad. Nauk. SSSR Ser. Mat.*, 36, 1173-1219(1972).

[6] L. A. Bokut, Imbeddings into simple associative algebras, *Algebra i Logika*, 15, 117-142(1976).

[7] L. A. Bokut Y. Fong and W.-F. Ke, Gröbner-Shirshov bases and composition lemma for associative conformal algebras: an example, *Contemporary Mathematics*, N 264, AMS, 63-91(2000).

[8] L. A. Bokut, L.-S. Shiao, Gröbner-Shirshov bases for Coxeter groups, *Communications in algebra*, 29, 4305-4319(2001).

[9] L. A. Bokut and K. P. Shum, Gröbner and Gröbner-Shirshov bases in algebra: an elementary approach, *SEA Bull. Math.*, 29, 227-252(2005).

[10] B. Buchberger, An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal [in German], Ph.D. thesis, University of Innsbruck, Austria, (1965).

[11] B. Buchberger, An algorithmical criteria for the solvability of algebraic systems of equations[in German], *Aequationes Math.*, 4, 374-383(1970).

[12] G. Higman, B. H. Neumann and H. Neumann, Embedding theorems for groups, *J. London Math. Soc.,* 24, 247-254(1949).

[13] N. Jacobson, Basic Algebra I, W. H.Freeman and Company, 1985.

[14] K. Kalorkoti, Decision problems in group theory, *Proc. Lond. Math. Soc., III. Ser.*, 44, 312-332(1982).

[15] R. C. Lyndon and P. E. Schupp, Combinatorial Group Theory, Springer-Verlag, 1977.

[16] P. S. Novikov, On algorithmic unsolvability of the problem of identity, *Dokl. Akad. Nauk SSSR*, 86, 709-712(1952).

[17] P. S. Novikov, Unsolvability of the conjugacy problem in the theory of groups, *Izv. Akad. Nauk SSSR Ser. Mat.*, 18, 485-524(1954).

[18] P. S. Novikov, On the algorithmic unsolvability of the word problem in group theory, *Trudy Mat. Inst. Steklov*, 44, 143(1955).

[19] A. I. Shirshov, Some algorithmic problem for Lie algebras, *Sibirsk. Mat. Z.*, 3(1962), 292-296(in Russian); English translation in SIGSAM Bull., 33(2), 3-6(1999).